SUBJECT: Director's speech on

8 Nov 71 at NSA during their

Security Week

Approved For Release 2003/02/27 : CIA-RDP84-00780R004300020001-4

SENDER WILL CHECK CLASSIFICATION TOP AND BOTTOM

UNCLASSIFIED | CONFIDENTIAL | SECRET

DD/S REGISTRY
FILE Speech

OFFICIAL ROUTING SLIP

TO	NAME AND ADDRESS	DATE	INITIALS
1	Executive Assistant to the Director Rm 7D6013		
2			
3			
4			
5			
6			

	ACTION		DIRECT REPLY		PREPARE REPLY
	APPROVAL		DISPATCH		RECOMMENDATION
	COMMENT		FILE		RETURN
	CONCURRENCE		INFORMATION		SIGNATURE

Remarks:

Dave -

Re our lunch chat -- the Director's text as we finally delivered it to him.

/s/ Bob

Robert S. Wattles

Att
Cy of text of Director's speech at NSA, 8 Nov 71

FOLD HERE TO RETURN TO SENDER

FROM: NAME, ADDRESS AND PHONE NO.	DATE
Assistant Deputy Director for Support 7D18, Hqs	13 NOV 71

UNCLASSIFIED | CONFIDENTIAL | SECRET

FORM NO. 1-67 237 Use previous editions (40)

ADD/S:RSW/ms (13 Nov 71)
Distribution:
Orig RS - Adse, w/cy of Att
1 - DD/S Subject, w/cy of Att ✓

8 November 1971

Good Afternoon,

I welcome the opportunity to participate in your Tenth Annual Security Week Program. In the climate of permissiveness and dissension that exists not only in this country but around the world, security must be a serious concern to us all.

The intelligence organizations of the Soviet Union and China, as well as those elsewhere in the Communist world, have become increasingly pervasive and sophisticated. One or more of them is active in every free world country. The KGB, of course, continues to be the most formidable of the Communist services, and our evidence indicates that it is steadily increasing its representation in non-Communist countries. The United States remains its top priority objective, and key elements of the American intelligence services, such as the FBI, the CIA, and NSA head its list of targets.

The number of Soviet officials assigned to the United States -- in the Embassy in Washington, in the Soviet Mission to the United Nations, and to various ancillary establishments, such as Tass -- has more than doubled over the past ten years. In September 1961, more than 900 such officials were present in this country. There are now more than 700. This increase is of serious concern, particularly when we know from a variety of reliable sources that more than 70 percent of the Soviets in the United States have some kind of intelligence mission. The pervasiveness of KGB operations was dramatized most recently in Britain in October when the British Foreign Office was forced to expel 90 Soviet representatives because of their intelligence activities and deny re-entry to some 15 others who were temporarily away from their posts.

Communist intelligence organizations are the major

problem, but in focussing on these we should not overlook the threat posed by our friends. It is all too easy to relax and slip into sloppy habits in our liaison activities. What we're doing, how we're doing it, and, obviously, what we know are of deep interest to all of them, be they the French, the Argentines, the Israelis, or the Belgians. Friendly services will probably not deliberately use our intelligence information against us, but it is obvious that we cannot depend on their discretion or their security in general. Courteous reticence should be the style of our intercourse.

In the face of these threats, I think it is important for all of us in intelligence work to periodically re-examine and re-evaluate our security practices to ensure that everything that can be done is being done to maintain the integrity of our intelligence mission.

There are many elements to security. If I were asked which is the most important, I would have to say that it is the security of personnel. It may be trite but it continues to be axiomatic that the security chain is only as strong as its weakest link. Despite the progress we have made in recent years in physical and technical security and despite the extensive precautions we have taken in other related fields, one "bad apple in the barrel" can cause extremely serious damage. You have all seen, over the years, tangible evidence that the United States intelligence community can be penetrated. Examples which show that "it can happen here" are well known to you all.

In the Central Intelligence Agency, we operate our personnel security program on the assumption that the Agency can be penetrated and we spend considerable time, in

conjunction with the FBI, in conducting investigations of alleged penetrations. Fortunately, the cases we have investigated thus far have always exonerated the employee. The fact that we have not yet found an agent of a foreign intelligence service at work in the Agency is fortunate, but it is significant only in so far as it acts as a spur to keep us attuned and alert to the ever present possibility that we may, in fact, have a spy in our midst. One's previous record means little the day the first agent is found.

At any rate, we must keep constantly in mind that because of current dissemination practices and the extensive coordination of both raw and finished intelligence, a penetration of any one agency usually involves the compromise of classified material of others. The Sgt. Johnson case is an example of this. Although he was assigned to the Armed

Forces Courier Service when he turned over classified information to the KGB, the material included sensitive reports of several agencies.

All of our intelligence organizations operate from the same basic framework in clearing employees. Our field investigations are generally thorough and comprehensive, and our security clearances are issued in accordance with the provisions of the same Executive Order. Personnel security, however, does not stop when an employee is safely on board. We cannot complacently assume that because our employees have been through security screening programs they will be good security risks during the rest of their careers. People change as they go along. Personal and financial problems occur, employees get tired of their jobs, others are frustrated, or develop on-job grievances of one kind or another. Most

people handle the inevitable personal and job-related problems intelligently and discreetly enough to keep these problems from assuming any security significance but a few others do not. It is those few who are most susceptible to attempts by the opposition at exploitation or penetration.

Of all the Americans known to have been successfully recruited by the KGB, none was ideologically motivated with the possible exception of the Rosenbergs. Rather, the Soviets have exploited a weakness of character, discretion or integrity, and the incidents have usually involved money, sex, revenge, or alcoholic problems.

Human weakness assumes even greater significance among our personnel abroad. The National Security Agency and CIA together staff installations in almost every country and these people overseas are obviously more exposed to the

painstaking surveillance of hostile intelligence services. We are all aware of recruitment attempts, kidnappings and even assassination. It behooves us to ensure that personnel assigned overseas are carefully screened from the outset and that they are continually indoctrinated in principles of personal security so that they are able to resist attempts at exploitation not only in this country, but in hostile environments as well.

Before leaving the subject of personnel security, I would like to stress a few factors which I believe can provide a basis for our continuing review of personnel security programs.

First, I would like to stress the importance of the supervisor. A supervisor who regards the people who work for him as human beings, subject to pressures, tension and stress - rather than simply as mechanical tools - is one of our strongest

security assets. I am not advocating a "buddy-buddy" or forced social relationship between supervisor and supervised. I am advocating that every supervisor know his people well enough that he can recognize changes in behavior patterns that may have potential security significance. Many of our supervisors have been able to detect and assist their employees with problems, which, if disregarded, might have worsened to the point where they could have become a definite security risk.

Secondly, and this is in accord with the theme of your program this year, it is important that a personnel security program be flexible. The young intelligence officers we are hiring today are just as sound as those we hired twenty years ago. Young people are needed, as they have always been needed, to inject the new ideas and imagination that will keep

United States intelligence on top of the ever increasing requirements. But we must recognize that the people we are hiring today have been raised and educated in a different world. We cannot force them into rigid patterns by regulation alone. We must, without any compromise of basic security standards, modify our regulations realistically and intelligently to reflect changing attitudes in changing times.

Finally, a good personnel security program must be administered with a positive tone, with liberal application of sympathy and human understanding. The most effective security service is one that is recognized as "friendly," whose first concern is the interest of the employees and the preservation of their human dignity. If the security service is administered in this fashion, employees will bring their problems to security personnel with confidence and trust.

A security service which loses sight of this has lost the race before it starts.

There is another area of security which has been of increasing concern in recent months. This is the frequent and extensive compromise of intelligence through unauthorized disclosures of classified information, primarily through the press. Since 1959, the Security Committee of the United States Intelligence Board has undertaken more than 100 investigations of newspaper and magazine articles which have contained classified intelligence information. This is a large number but more disturbing is the fact that 22 of these have occurred in the first five months of 1971, much the highest rate for any equivalent period in the history of the intelligence community.

What is the effect of these disclosures and what is their significance to us as professional intelligence officers?

Obviously, this free flow of classified information gives the Soviet Union and other foreign powers gratuitous insight into our intelligence capabilities and limitations. Equally important, it serves to undermine at all levels of government the importance of maintaining security.

It is extremely difficult and usually impossible to conduct a successful investigation of unauthorized disclosures. The chief problem is the wide dissemination of intelligence products both within the intelligence community and elsewhere in Government. In many cases a thorough security investigation would involve interviewing literally thousands of individual consumers.

Thus, we have had to turn to other means of tightening our security and maintaining the integrity of our intelligence information. Over the years, I have given considerable thought

to the reasons for damaging disclosures. Some of them occur, of course, during periods of national debate over significant and controversial issues, and stem directly from attempts to use classified information to influence major policy. One can understand the deep commitment loyal government employees may have to particular policy positions, but, in my mind, the use of sensitive intelligence in this way is inevitably short-sighted. One almost certainly gives away more to foreign powers in useful intelligence about us than one gains in leverage one way or the other on the domestic legislative process. But aside from this I will never be able to accept the more general and fundamental concept that one individual can assume responsibility for deciding that he alone knows best what is in the national interest.

The President has expressed grave concern about the

proliferation of unauthorized disclosures. He has charged all United States departments and agencies with the responsibility for taking action. Specifically, he has directed that immediate review be made of all personnel having special or compartmented clearances with a view toward reducing the number of these clearances to an absolute minimum consistent with "need-to-know." He has also created a special committee to review and recommend changes in the Executive Order - number 10501 - which contains procedures governing the classification and declassification of documents in the United States Government.

As the Chairman of the United States Intelligence Board and as Director of Central Intelligence, I have taken a number of actions to close this gap in the security of the intelligence community. I have made repeated requests to members of the

heard that requirements for the dissemination of intelligence information continually be reviewed and limited; that special clearances be held to the minimum; and that personnel be re-indoctrinated periodically on the need for security. I hope that these actions have had some effect but in the final analysis each individual employee who has access to classified intelligence information must take upon himself the responsibility for ensuring that he maintains the integrity of the privileged information to which he has access. Unauthorized disclosures obviously must stop. I urge each of you to assume this responsibility fully. Security is indispensible to the United States intelligence community and to the Government. We must work individually and collectively to maintain the most impeccable standards.